REMARKS

Claims 1-15 and 17-20 have been canceled above. Independent program product claim 16 has been amended, and new dependent program product claims 21-25 have been entered above. Independent system claim 26 has been added and corresponds to claim 16. New dependent system claims 27-31 correspond to dependent program product claims 21-25. New program product claims 32-37 have been added. Independent claim 32 includes some, but not all features of claim 16.

Claim 16 was rejected under 35 USC 102(e) based on US 1003/0217039 by Kurtz et al. Claims 2, 3, 11-15, 17 and 20 were rejected under 35 USC 103(a) based on Kurtz et al. and US 2003/0217039 by Chandrashekhar et al. Applicant respectfully traverses this rejection based on the following.

Claim 16 recites a combination of security functions not found in the prior art. More specifically, claim 16 recites program instructions to review **security of an authentication computer from attack, the authentication computer residing** within the network perimeter and authenticating users outside of the network perimeter that request access to an application within the network perimeter. Thus, claim 16 recites program instructions to review security **of an authentication computer** within the perimeter. This corresponds to original claim 2, against which the Examiner cited Paragraph [0032] of Chandrashekhar et al. Chandrashekhar et al. teaches security of an application by authentication of the requestor before access to the application, **but not reviewing security of the authentication computer (itself) from attack**, as recited in claim 16. More specifically, Chandrashekhar et al. teaches,

> "There are at least three potential targets for security attacks; namely, the ASP customer, the ASP and the Service Provider. Therefore, preferably, Service Providers and ASPs enter into a partnership that defines their respective security responsibilities to ensure that the eight security countermeasure mechanisms are all in place on a **per-application basis**.

Table 1 provides some examples of how the Security Mechanisms **are applied** to the Security Layers. Examples can be identified for all three security planes: end-user, control, and management.

TABLE 1			
Security Layer			
Security Mechanism	Infrastructure	Services	Applications
Access Management	Controls access to	Controls access to	Controls access to
individual network	network services.	network-based	
elements or	applications.		
transmission facilities.			
Authentication	Confirms identify of	Confirms identify of	Confirms identify of
person attempting to	person attempting to	person attempting to	
access individual	access network services.	access network	
network elements or	applications.		
transmission facilities.			
Non-repudiation	Maintains a record of	Maintains a record of	Maintains a record of
activities performed by	activities performed by	activities performed by	
each person who has	each person who has	each person who has	
accessed individual	accessed network	accessed network	
network elements or	services.	applications.	
transmission facilities.			
Data Confidentiality	Protection against the	Protection against the	Protection against the
unauthorized reading of	unauthorized reading of	unauthorized reading of	
data stored on	data as it traverses the	data as it is being	
individual boxes.	network.	processed or generated	
by an application.			
Communication	Protection against the	Data is not diverted	Data is only

TABLE 1			
		or	transmitted
Security	incorrect installation of	intercepted as it	between authorized
cables.	traverses the network.	applications and	
endpoints.			
Integrity	Protection against	Protection against	Protection against
unauthorized creation,	unauthorized creation,	unauthorized creation,	
modification, deletion	modification, deletion	modification, deletion	
of data stored on	of data as it traverses	of data by applications.	
individual network	the network.		
elements.			
Availability	Individual network	Network Service is	Application is available.
element is available.	available.		
Privacy	Information about	Information about	Information about
individual network	services being used by	applications being	
elements (e.g., IP	end-users is kept	accessed by end-users is	
addresses) is kept	private.	kept private.	
private.			

> **Three types of activities are performed over the Infrastructure, Services and Applications security layers.** These activities are represented by three planes; namely the Management Plane **120**MP, the Control Plane **120**CP, and the End-user Plane **120**EUP. **The protection provided by the eight mechanisms of security countermeasures is provided to each of these types of activities.** The management plane **120**MP is adapted to operations, administration, maintenance, provisioning and other management functions associated with the network elements, transmission facilities, operations support systems and the like." (emphasis added) Chandrashekhar et al. Paragraphs [0031-0033].

Thus, Chandrashekhar et al. teaches security of an application by authentication of the requestor before access to the application, **but not reviewing security of the authentication computer (itself) from attack**, as recited in claim 16. Kurtz et al. does not fill the foregoing gap of Chandrashekhar et al.

Kurtz et al. pertain to assessing network vulnerability, and includes various processes including port scanning to determine what network addresses are active, and what ports at those addresses are active, a vulnerability assessment of vulnerabilities of the ports and vulnerability scripts that apply known vulnerabilities to open ports of the live target computers. More specifically, Kurtz et al. teaches,

> "The present invention solves these problems and more through a comprehensive network vulnerability testing and reporting method and system. Specifically, the testing system features include a selected combination of: (1) a non-destructive identification of target computer operating system; (2) **a multiple-tier port scanning method for determination of what network addresses are active and what ports are active at those addresses**; (3) a comparison of collected information about the target network with a database of known vulnerabilities; (4) **a vulnerability assessment of some vulnerabilities on identified ports of identified target computers**; (5) an active assessment of vulnerabilities reusing data discovered from previously discovered target computers; (6) an application of a quantitative score to objectively and comparatively rank the security of the target network; and, (7) reduction of detailed results of the information collected into hierarchical, dynamic and graphical representations of the target network, target computers, and vulnerabilities found therein." (emphasis added) Kurtz et al. Paragraph [0011]

> "After completing the TCP traceroute routine **362**, the method proceeds to the vulnerability assessment routine **364**. As described in more detail below, in the vulnerability assessment routine **364**, **the method executes vulnerability scripts that apply known vulnerabilities to open ports of the live target computers to determine whether the ports of the target computers exhibit the potential vulnerabilities**. The method uses information stored in a known vulnerability database **366** to select the vulnerability scripts to executes for each active port. Information collected from vulnerable target computers is advantageously stored to the target computer database **344**." (emphasis added) Kurtz et al. Paragraph [0087]

> "In one embodiment, the vulnerability assessment routine **364** preferably only performs vulnerability checks associated with the identified operating system and open ports of the target computer as determined by the operating system identification routine **350** and service discovery routine **340**. If the operating system is not conclusively identified, typically the routine runs all known vulnerabilities for the open ports of the target computer." Kurtz et al. Paragraph [0088]

Thus, Kurtz et al. pertain to assessing network vulnerability, and includes various processes including port scanning to determine what network addresses are active, and what ports at those addresses are active, a vulnerability assessment of vulnerabilities of the ports and vulnerability scripts that apply known vulnerabilities to open ports of the live target computers. However, Kurtz et al. does not teach or suggest review of security of the authentication computer (itself) from attack, as recited in claim 16. Therefore, Kurtz et al. in combination with Chandrashekhar et al. fail to teach or suggest a key feature of claim16, and do not form a prima facie case of obviousness.

Claims 21-25 depend on claim 16, and therefore, distinguish over the prior art for the same reasons that claim 16 distinguishes thereover.

Claim 21 further distinguishes over the prior art by the recitation of program instructions to assess protection by the firewall against probing into the network perimeter based in part on the message flow rules of the firewall. This is specifically directed to detection of vulnerability to **probing** apart from vulnerability to subsequent related attack.

Claim 25 further distinguishes over the prior art by the recitation of program instructions to review security of the application that transfers data across the network perimeter based on **a location of data transferred by the application**.

Independent claim 26 distinguishes over the prior art for the same reasons that claim 16 distinguishes thereover.

Claims 27-31 depend on claim 26, and therefore, distinguish over the prior art for the same reasons that claim 26 distinguishes thereover.

Claim 27 further distinguishes over the prior art for the same reasons that claim 21 further distinguishes thereover.

Claim 31 further distinguishes over the prior art for the same reasons that claim 25 further distinguishes thereover.

Independent claim 32, which is broader than independent claim 16, distinguishes over the prior art for the same reason that claim 16 distinguishes thereover, i.e. Kurtz et al. and Chandrashekhar et al. do not teach or suggest review of security of the authentication computer (itself) from attack.

Claims 33-37 depend on claim 32, and therefore, distinguish over the prior art for the same reasons that claim 32 distinguishes thereover.

Claim 33 further distinguishes over the prior art for the same reasons that claim 21 further distinguishes thereover.

Claim 34 further distinguishes over the prior art for the same reasons that claim 25 further distinguishes thereover.

Based on the foregoing, Applicant requests allowance of the present patent application as amended above.

Respectfully submitted,

Dated:_April 20, 2011	/Arthur J. Samodovitz/__
Phone:607-429-4368	Arthur J. Samodovitz
Fax: 607-429-4119	Reg. No. 31,297